TO: Agency Chief Information Officers **DRAFT 1/23/03**

FROM: William Hadesty
Associate Chief Information Officer
Office of Cyber Security

SUBJECT: 2003 Annual Security Plans for Information Technology (IT) Systems, CS-021

This memorandum initiates the annual call for the USDA 2003 Annual Security Plans for Information Technology (IT) Systems. Information security has escalated as the subject of high-level attention from both the press and media. Recent terrorist attacks have only highlighted the need to ensure that we have the highest level of information security practices. IT Security Plans have become the foundation document in the overall security process because they define the system security features and controls. They support Capital Planning and Investment Control (CPIC), Federal Information Security Management Act (FISMA) reporting, System Life Cycle efforts, Risk Management activities as well as the Certification and Accreditation of Information Technology (IT) systems. Therefore, it is critical that they be prepared/updated on a annual basis with the most current information concerning each agency's information security practices. All plans and supporting material prepared for this request are due to my office no later than **April 30, 2003**.

The Computer Security Act of 1987 and Departmental Manual 3140-1 require Annual Security Plans for IT Systems. Each plan should reflect accurate and comprehensive details required by OMB Circular A-130 and NIST 800-18, Guide for Developing Security Plans for IT Systems. **Each agency is required to address the specifics of security control and establish responsibility for ensuring those controls function as intended and to include information on all weakness identified for correction during the 2001 Annual Security Plan review.** We will send agencies the Security Plan Review Comments from 2001, upon request, if for some reason you are unable to locate them. Agency plans will be subject to CS on-site review for veracity and accuracy in reporting. Results of the on-site reviews will be provided to each Agency Head.

The generic term "system" covers all General Support Systems (GSS) and Major Applications. Security plans for other applications are not required because the security controls for these applications would be provided by the GSS in which they operate. Each agency should develop an Overall Security Program plan and individual plans for each GSS and Major Applications. CS has provided templates for these three types of plans. In many cases information required by these templates is already available from prior submissions, therefore can be updated and included in new submissions. This year our guidance package also includes a section to assist agencies in defining GSS and Major Applications and modified templates for electronic submission of plans. Modification of the templates closely parallels NIST 800-18 but also contains information required by FISMA and the Office of Inspector General audits.

As we have in previous years, the Agency Head or Administrator must submit these plans by cover letter in which they will be attesting to the completeness and accuracy of the security plan submissions. This memo will also include information on whether the material weaknesses identified in the 2001 Annual Security Plan review have been corrected or if there is an Action Plan and Milestones in the FISMA, Plan of Action and Milestone Report for any weaknesses still outstanding. These plans will also be used as a basis for security recommendations under the CPIC process to the Executive Information Technology Investment Review Board (EITIRB) who approves funding. Recommendations from my office could include holding the investment in its current phase, unfavorable security comments or loss of funding.

My office still requires that an Overall Agency Security Program Plan be submitted. This plan serves as the master document under which all GSS and Major Application Plans rest. This plan should reflect all those efforts that occur at a program level such as: Security Program Functions, Program Security Training and Awareness, Security Performance Measures for the Program, Long-Term Strategy, Personnel Security for the Program, and Program Risk Assessment Information. This information is not covered by plans for GSS or Major Applications, but is essential in determining agency progress in implementing an acceptable overall security program. Again, Annual Security Plans for Information Technology (IT) Systems are due to my office by **April 30, 2003**.

Please contact myself on (202) 690-0048/E-mail at bill.hadesty@usda.gov or Rick Perry, Information Security Specialist, on (202) 690-3230/E-mail at rl.perry@usda.gov with any questions or concerns. We appreciate the effort and support of you and your staff in this important endeavor.

Attachments